



Threats and Countermeasures Breakout Session

Bojan Cukic

Center for Identification Technology Research
West Virginia University

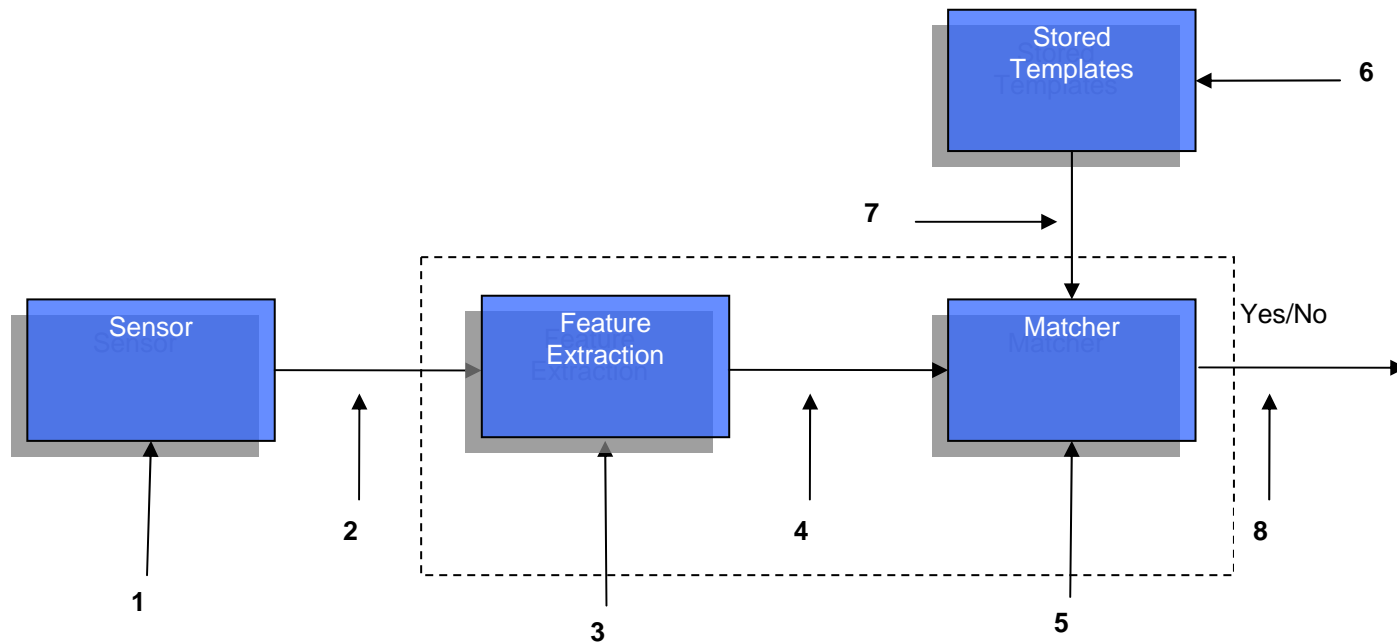
*Workshop on Biometrics and E-Authentication
Over Open Networks*
March 2005



Session Scope



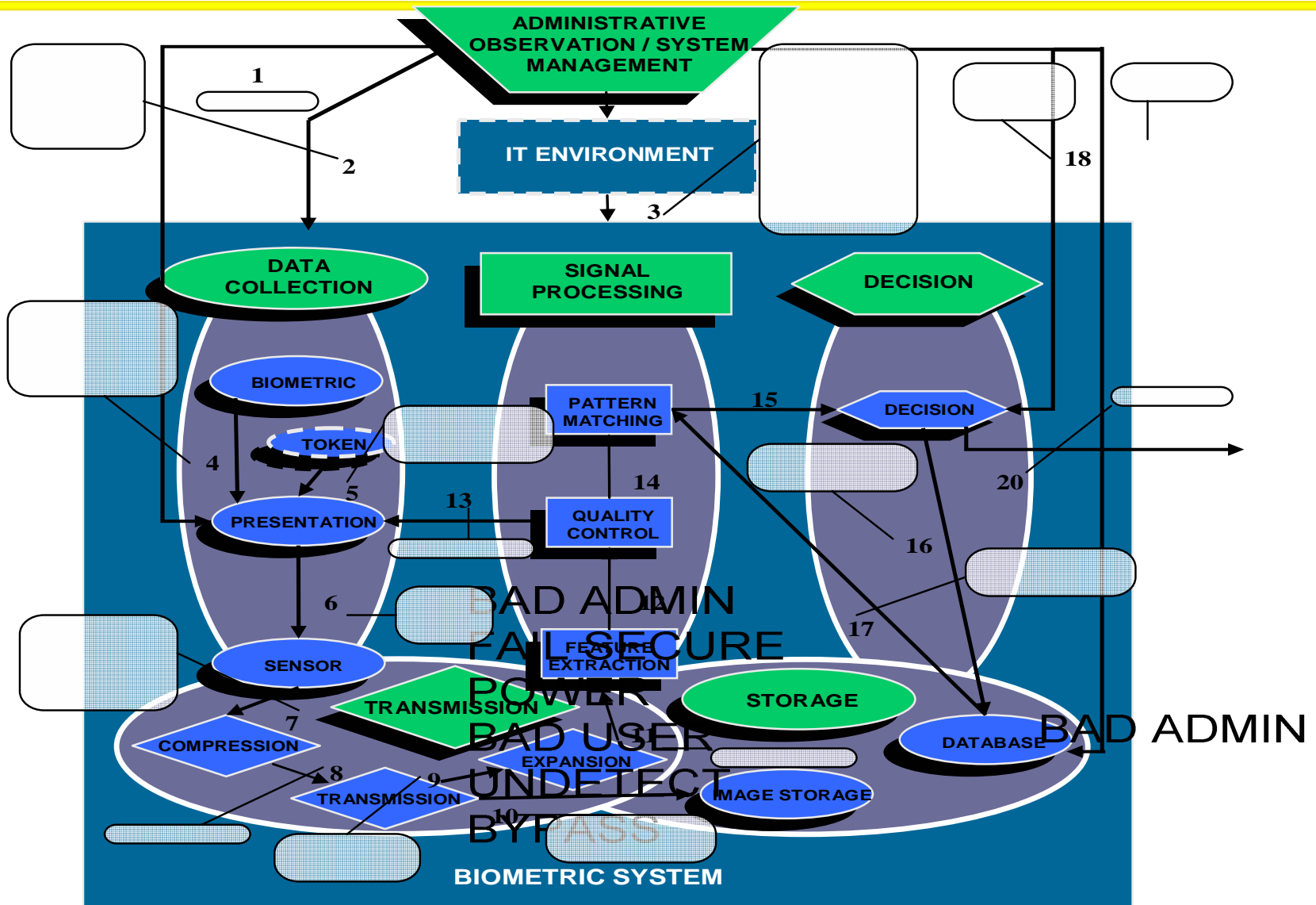
- *Threat*
 - An expression of intent to do harm (Webster).
 - Circumstances that make attacks likely to occur, system vulnerabilities exposed.
- *Vulnerability*
 - Weakness of protection that might be exploited.
 - *Attacks* exploit vulnerabilities.
- *Countermeasures*
 - Controls and preventive measures countering the threats.



- | | |
|--|--|
| 1. Spoofing | 5. Corrupting the matcher |
| 2. Sensor Bypass | 6. Unauthorized access to stored templates |
| 3. Overriding feature extraction | 7. Corruption of template fetching |
| 4. Tampering with feature representation | 8. Decision override. |



- Scale
 - Biometric access points
 - Number of enrolled users
- Heterogeneity
 - Biometric (sub)systems and modalities
 - Algorithms
 - Template storage
- Decentralization
 - System-wide control
 - Template acquisition, storing and matching
- Inter- and intra-networking
- Web-enabled or Web-adverse



Who Goes There?: Authentication Through the Lens of Privacy, National Academy Press, 2003

Recommendation regarding the future use of Biometrics:

Biometric Technologies should not be used to authenticate users via Remote authentication servers because of the potential for large-scale Privacy and security compromises in the event of a successful attack (either internal or external) against such servers. The use of biometrics For local authentication – for example, to control access to a private key on a smart card – is a more appropriate type of use for biometrics.

In the biometrics community:

- Vendor enthusiasm
 - Increasing product maturity
- Research advances
- Many parallel studies
 - Whither Biometrics

In the society:

- Perceptions
 - Expectations, publicity.
- Privacy climate
- Legal doctrine



- Identify and prioritize threats

$$RISK = Occurance_Likelihood \otimes Consequence_Severity$$

- Discuss the maturity of countermeasures
- Identify gaps
 - State of knowledge vs. state of practice
 - Lack or abundance of practical solutions
 - Lack of knowledge
- Suggest agenda
 - Common needs
 - Priorities